

**Method and apparatus for encrypting and decrypting data using
encryption key contained in electronic watermark**

Patent Number: ☐ [US2002108043](#)
Publication date: 2002-08-08
Inventor(s): TANAKA NOBUYUKI (JP)
Applicant(s): NIPPON ELECTRIC CO (JP)
Requested Patent: ☐ [JP2002232412](#)
Application Number: US20020057521 20020124
Priority Number(s): JP20010027207 20010202
IPC Classification: H04L9/00
EC Classification: [H04L9/08](#)
Equivalents:

Abstract

In encoder side, an electronic watermark generating device generates an electronic watermark which contains an encryption key. An electronic watermark inserting device inserts the electronic watermark containing the encryption key into a first portion of data. An encrypting device encrypts a second portion of the data with the encryption key. The first portion into which the watermark containing the encryption key has been inserted and the second portion which has been encrypted with the encryption key are combined by a switch and thereafter recorded on a record medium or transmitted to a network. In decoder side, the watermark containing the encryption key is extracted from the first portion and the encryption key is extracted from the watermark. The second portion is decrypted with the extracted encryption key.

Data supplied from the esp@cenet database - 12

特開2002-232412

(P 2 0 0 2 - 2 3 2 4 1 2 A)

(43)公開日 平成14年8月16日(2002.8.16)

(51)Int. C1.7		識別記号	F I		モード(参考)	
H 0 4 L	9/08		G 0 6 T	1/00	5 0 0 B	5B057
G 0 6 T	1/00	5 0 0	G 0 9 C	5/00		5C063
G 0 9 C	5/00		G 1 1 B	20/10	H	5C064
G 1 0 L	11/00		H 0 4 N	1/387		5C076
	19/00		H 0 4 L	9/00	6 0 1 B	5D044
審査請求	未請求	請求項の数75	OL		(全20頁)	最終頁に続く

(21)出願番号 特願2001-27207(P2001-27207)

(22)出願日 平成13年2月2日(2001.2.2)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 田中 信行

東京都港区芝五丁目7番1号 日本電気株式
会社内

(74)代理人 100065385

弁理士 山下 穰平

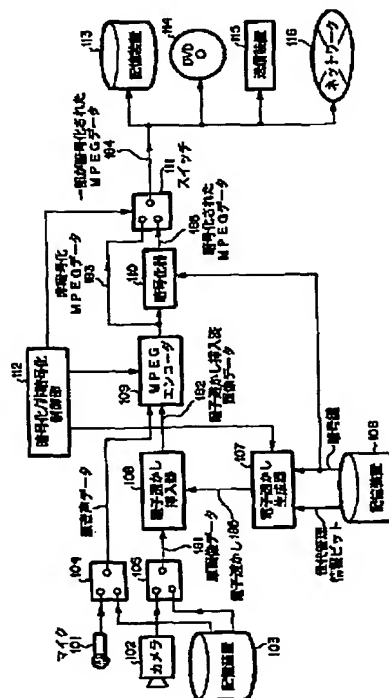
[最終頁に続く](#)

(54)【発明の名称】電子透かしに含めた暗号鍵を用いた暗号化装置及び復号化装置並びにそれらの方法

(57) 【要約】

【課題】 電子透かし技術と、暗号化技術のそれぞれの特徴を活かし、それらを組み合わせることにより、よりセキュアなデジタルコンテンツの再生制限をすること可能とする。

【解決手段】 暗号化装置は、第1の暗号鍵を含んだ第1の電子透かしを生成する生成手段と、データの第1の部分に第1の暗号鍵を含んだ第1の電子透かしを挿入する電子透かし挿入手段と、データの第2の部分を第1の暗号鍵で暗号化する暗号化手段と、を備える。復号化装置は、データの第1の部分より第1の電子透かしを検出する電子透かし検出手段と、第1の電子透かしより第1の暗号鍵を抽出する暗号鍵抽出手段と、データの第2の部分を第1の暗号鍵で暗号解読する暗号解読手段と、を備える。



【特許請求の範囲】

【請求項 1】 第 1 の暗号鍵を含んだ第 1 の電子透かしを生成する生成手段と、
データの第 1 の部分に前記第 1 の暗号鍵を含んだ前記第 1 の電子透かしを挿入する電子透かし挿入手段と、
前記データの第 2 の部分を前記第 1 の暗号鍵で暗号化する暗号化手段と、
を備えることを特徴とする電子透かしに含めた暗号鍵を用いた暗号化装置。

【請求項 2】 請求項 1 に記載の暗号化装置において、
前記電子透かし生成手段は、第 2 の暗号鍵を含んだ第 2 の電子透かしを生成し、
前記電子透かし挿入手段は、前記第 2 の部分が前記暗号化手段により前記第 1 の暗号鍵で暗号化される前に、前記第 2 の部分に前記第 2 の電子透かしを挿入し、
前記暗号化手段は、前記データの第 3 の部分を前記第 2 の暗号鍵で暗号化することを特徴とする暗号化装置。

【請求項 3】 請求項 1 に記載の暗号化装置において、
前記電子透かし生成手段は、第 n (n は 1 より大きい整数) の暗号鍵を含んだ第 n の電子透かしを生成し、
前記電子透かし挿入手段は、第 n の部分が前記暗号化手段により第 $(n-1)$ の暗号鍵で暗号化される前に、前記第 n の部分に前記第 n の電子透かしを挿入し、
前記暗号化手段は、前記データの第 $(n+1)$ の部分を前記第 n の暗号鍵で暗号化することを特徴とする暗号化装置。

【請求項 4】 請求項 1 に記載の暗号化装置において、
前記データを圧縮する圧縮手段を更に備えることを特徴とする暗号化装置。

【請求項 5】 請求項 4 に記載の暗号化装置において、
前記圧縮手段は、前記データを暗号化する前に、前記データを圧縮することを特徴とする暗号化装置。

【請求項 6】 請求項 1 に記載の暗号化装置において、
前記データは画像データ、音声データ及び文字データの少なくとも 1 つを含むことを特徴とする暗号化装置。

【請求項 7】 請求項 1 に記載の暗号化装置において、
前記第 1 の部分と前記第 2 の部分は同一の媒体から出力されることを特徴とする暗号化装置。

【請求項 8】 請求項 1 に記載の暗号化装置において、
前記第 2 の部分は前記第 1 の部分と異なった媒体から出力されることを特徴とする暗号化装置。

【請求項 9】 請求項 1 に記載の暗号化装置において、
前記第 1 の部分はコマーシャルを含むことを特徴とする暗号化装置。

【請求項 10】 データの第 1 の部分より第 1 の電子透かしを検出する電子透かし検出手段と、
前記第 1 の電子透かしより第 1 の暗号鍵を抽出する暗号鍵抽出手段と、
前記データの第 2 の部分を前記第 1 の暗号鍵で暗号解読する暗号解読手段と、

を備えることを特徴とする電子透かしに含めた暗号鍵を用いた復号化装置。

【請求項 11】 請求項 10 に記載の復号化装置において、
前記電子透かし検出手段は、前記暗号解読手段により前記第 1 の暗号鍵で暗号解読された前記第 2 の部分より第 2 の電子透かしを検出し、
前記暗号鍵抽出手段は、前記第 2 の電子透かしより第 2 の暗号鍵を抽出し、
前記暗号解読手段は、前記データの第 3 の部分を前記第 2 の暗号鍵で暗号解読することを特徴とする復号化装置。

【請求項 12】 請求項 10 に記載の復号化装置において、
前記電子透かし検出手段は、前記暗号解読手段により第 $(n-1)$ (n は 1 より大きい整数) の暗号鍵で暗号解読された第 n の部分より第 n の電子透かしを検出し、
前記暗号鍵抽出手段は、前記第 n の電子透かしより第 n の暗号鍵を抽出し、
前記暗号解読手段は、前記データの第 $(n+1)$ の部分を前記第 n の暗号鍵で暗号解読することを特徴とする復号化装置。

【請求項 13】 請求項 10 に記載の復号化装置において、
前記データを伸長する伸長手段を更に備えることを特徴とする復号化装置。

【請求項 14】 請求項 13 に記載の復号化装置において、
前記伸長手段は、前記データが暗号解読された後に、前記データを伸長することを特徴とする復号化装置。

【請求項 15】 請求項 10 に記載の復号化装置において、
前記データは画像データ、音声データ及び文字データの少なくとも 1 つを含むことを特徴とする復号化装置。

【請求項 16】 請求項 10 に記載の復号化装置において、
前記第 1 の部分と前記第 2 の部分は同一の媒体から入力されることを特徴とする復号化装置。

【請求項 17】 請求項 10 に記載の復号化装置において、
前記第 2 の部分は前記第 1 の部分と異なった媒体から入力されることを特徴とする復号化装置。

【請求項 18】 請求項 10 に記載の復号化装置において、
前記第 1 の部分はコマーシャルを含むことを特徴とする復号化装置。

【請求項 19】 第 1 の暗号鍵を含んだ第 1 の電子透かしを生成するステップと、
データの第 1 の部分に前記第 1 の暗号鍵を含んだ前記第 1 の電子透かしを挿入するステップと、
前記データの第 2 の部分を前記第 1 の暗号鍵で暗号化するステップと、

を有することを特徴とする電子透かしに含めた暗号鍵を

用いた暗号化方法。

【請求項 20】 請求項 19 に記載の暗号化方法において、
第 2 の暗号鍵を含んだ第 2 の電子透かしを生成するステップと、
前記第 2 の部分が前記第 1 の暗号鍵で暗号化される前に、前記第 2 の部分に前記第 2 の電子透かしを挿入するステップと、
前記データの第 3 の部分を前記第 2 の暗号鍵で暗号化するステップと、
を更に有することを特徴とする暗号化方法。

【請求項 21】 請求項 19 に記載の暗号化方法において、
第 n (n は 1 より大きい整数) の暗号鍵を含んだ第 n の電子透かしを生成するステップと、
第 n の部分が前記暗号化手段により第 $(n-1)$ の暗号鍵で暗号化される前に、前記第 n の部分に前記第 n の電子透かしを挿入するステップと、
前記データの第 $(n+1)$ の部分を前記第 n の暗号鍵で暗号化するステップと、
を更に有することを特徴とする暗号化方法。

【請求項 22】 請求項 19 に記載の暗号化方法において、
前記データを圧縮するステップを更に備えることを特徴とする暗号化方法。

【請求項 23】 請求項 22 に記載の暗号化方法において、前記データを暗号化する前に、前記データを圧縮することを特徴とする暗号化方法。

【請求項 24】 請求項 19 に記載の暗号化方法において、前記データは画像データ、音声データ及び文字データの少なくとも 1 つを含むことを特徴とする暗号化方法。

【請求項 25】 請求項 19 に記載の暗号化方法において、
前記第 1 の部分を媒体に出力するステップと、
前記第 2 の部分を前記媒体と同一の媒体に出力するステップと、
を更に有することを特徴とする暗号化方法。

【請求項 26】 請求項 19 に記載の暗号化方法において、
前記第 1 の部分を媒体に出力するステップと、
前記第 2 の部分を前記媒体と異なった媒体に出力するステップと、
を更に有することを特徴とする暗号化方法。

【請求項 27】 請求項 19 に記載の暗号化方法において、前記第 1 の部分はコマーシャルを含むことを特徴とする暗号化方法。

【請求項 28】 データの第 1 の部分より第 1 の電子透かしを検出するステップと、
前記第 1 の電子透かしより第 1 の暗号鍵を抽出するステ

ップと、
前記データの第 2 の部分を前記第 1 の暗号鍵で暗号解読するステップと、
を有することを特徴とする電子透かしに含めた暗号鍵を用いた復号化方法。

【請求項 29】 請求項 28 に記載の復号化方法において、
前記第 1 の暗号鍵で暗号解読された前記第 2 の部分より第 2 の電子透かしを検出するステップと、
前記第 2 の電子透かしより第 2 の暗号鍵を抽出するステップと、
前記データの第 3 の部分を前記第 2 の暗号鍵で暗号解読するステップと、
を更に有することを特徴とする復号化方法。

【請求項 30】 請求項 28 に記載の復号化方法において、
第 $(n-1)$ (n は 1 より大きい整数) の暗号鍵で暗号解読された第 n の部分より第 n の電子透かしを検出するステップと、
前記第 n の電子透かしより第 n の暗号鍵を抽出するステップと、
前記データの第 $(n+1)$ の部分を前記第 n の暗号鍵で暗号解読するステップと、
を更に有することを特徴とする復号化方法。

【請求項 31】 請求項 28 に記載の復号化方法において、
前記データを伸長するステップを更に有することを特徴とする復号化方法。

【請求項 32】 請求項 31 に記載の復号化方法において、前記データが暗号解読された後に、前記データを伸長することを特徴とする復号化方法。

【請求項 33】 請求項 28 に記載の復号化方法において、前記データは画像データ、音声データ及び文字データの少なくとも 1 つを含むことを特徴とする復号化方法。

【請求項 34】 請求項 28 に記載の復号化方法において、
前記第 1 の部分を媒体から入力するステップと、
前記第 2 の部分を前記媒体と同一の媒体から入力するステップと、
を更に有することを特徴とする復号化方法。

【請求項 35】 請求項 28 に記載の復号化方法において、
前記第 1 の部分を媒体から入力するステップと、
前記第 2 の部分を前記媒体と異なった媒体から入力するステップと、
を更に有することを特徴とする復号化方法。

【請求項 36】 請求項 28 に記載の復号化方法において、前記第 1 の部分はコマーシャルを含むことを特徴とする復号化方法。

10

20

30

40

50

【請求項 3 7】 第 1 の暗号鍵を含んだ第 1 の電子透かしを生成するステップと、
データの第 1 の部分に前記第 1 の暗号鍵を含んだ前記第 1 の電子透かしを挿入するステップと、
前記データの第 2 の部分を前記第 1 の暗号鍵で暗号化するステップと、
を有することを特徴とする電子透かしに含めた暗号鍵を用いた暗号化方法をコンピュータに実行させるためのコンピュータプログラム。

【請求項 3 8】 請求項 3 7 に記載のコンピュータプログラムにおいて、
前記暗号化方法は、
第 2 の暗号鍵を含んだ第 2 の電子透かしを生成するステップと、
前記第 2 の部分が前記第 1 の暗号鍵で暗号化される前に、前記第 2 の部分に前記第 2 の電子透かしを挿入するステップと、
前記データの第 3 の部分を前記第 2 の暗号鍵で暗号化するステップと、
を更に有することを特徴とするコンピュータプログラム。

【請求項 3 9】 請求項 3 7 に記載のコンピュータプログラムにおいて、
前記暗号化方法は、
第 n (n は 1 より大きい整数) の暗号鍵を含んだ第 n の電子透かしを生成するステップと、
第 n の部分が前記暗号化手段により第 $(n-1)$ の暗号鍵で暗号化される前に、前記第 n の部分に前記第 n の電子透かしを挿入するステップと、
前記データの第 $(n+1)$ の部分を前記第 n の暗号鍵で暗号化するステップと、
を更に有することを特徴とするコンピュータプログラム。

【請求項 4 0】 請求項 3 7 に記載のコンピュータプログラムにおいて、
前記暗号化方法は、
前記データを圧縮するステップを更に備えることを特徴とするコンピュータプログラム。

【請求項 4 1】 請求項 4 0 に記載のコンピュータプログラムにおいて、前記暗号化方法は、前記データを暗号化する前に、前記データを圧縮することを特徴とするコンピュータプログラム。

【請求項 4 2】 請求項 3 7 に記載のコンピュータプログラムにおいて、前記データは画像データ、音声データ及び文字データの少なくとも 1 つを含むことを特徴とするコンピュータプログラム。

【請求項 4 3】 請求項 3 7 に記載のコンピュータプログラムにおいて、
前記暗号化方法は、
前記第 1 の部分を媒体に出力するステップと、

前記第 2 の部分を前記媒体と同一の媒体に出力するステップと、
を更に有することを特徴とするコンピュータプログラム。

【請求項 4 4】 請求項 3 7 に記載のコンピュータプログラムにおいて、
前記暗号化方法は、
前記第 1 の部分を媒体に出力するステップと、
前記第 2 の部分を前記媒体と異なった媒体に出力するステップと、
を更に有することを特徴とするコンピュータプログラム。

【請求項 4 5】 請求項 3 7 に記載のコンピュータプログラムにおいて、前記第 1 の部分はコマーシャルを含むことを特徴とするコンピュータプログラム。

【請求項 4 6】 データの第 1 の部分より第 1 の電子透かしを検出するステップと、
前記第 1 の電子透かしより第 1 の暗号鍵を抽出するステップと、
前記データの第 2 の部分を前記第 1 の暗号鍵で暗号解読するステップと、
を有することを特徴とする電子透かしに含めた暗号鍵を用いた復号化方法をコンピュータに実行させるためのコンピュータプログラム。

【請求項 4 7】 請求項 4 6 に記載のコンピュータプログラムにおいて、
前記暗号化方法は、
前記第 1 の暗号鍵で暗号解読された前記第 2 の部分より第 2 の電子透かしを検出するステップと、
前記第 2 の電子透かしより第 2 の暗号鍵を抽出するステップと、
前記データの第 3 の部分を前記第 2 の暗号鍵で暗号解読するステップと、
を更に有することを特徴とするコンピュータプログラム。

【請求項 4 8】 請求項 4 6 に記載のコンピュータプログラムにおいて、
前記暗号化方法は、
第 $(n-1)$ (n は 1 より大きい整数) の暗号鍵で暗号解読された第 n の部分より第 n の電子透かしを検出するステップと、
前記第 n の電子透かしより第 n の暗号鍵を抽出するステップと、
前記データの第 $(n+1)$ の部分を前記第 n の暗号鍵で暗号解読するステップと、
を更に有することを特徴とするコンピュータプログラム。

【請求項 4 9】 請求項 4 6 に記載のコンピュータプログラムにおいて、
前記暗号化方法は、

前記データを伸長するステップを更に有することを特徴とするコンピュータプログラム。

【請求項50】 請求項49に記載のコンピュータプログラムにおいて、前記暗号化方法は、前記データが暗号解読された後に、前記データを伸長することを特徴とするコンピュータプログラム。

【請求項51】 請求項46に記載のコンピュータプログラムにおいて、前記データは画像データ、音声データ及び文字データの少なくとも1つを含むことを特徴とするコンピュータプログラム。

【請求項52】 請求項46に記載のコンピュータプログラムにおいて、前記暗号化方法は、前記第1の部分を媒体から入力するステップと、前記第2の部分を前記媒体と同一の媒体から入力するステップと、を更に有することを特徴とするコンピュータプログラム。

【請求項53】 請求項46に記載のコンピュータプログラムにおいて、前記暗号化方法は、前記第1の部分を媒体から入力するステップと、前記第2の部分を前記媒体と異なった媒体から入力するステップと、を更に有することを特徴とするコンピュータプログラム。

【請求項54】 請求項46に記載のコンピュータプログラムにおいて、前記第1の部分はコマーシャルを含むことを特徴とするコンピュータプログラム。

【請求項55】 第1の暗号鍵を含んだ第1の電子透かしを生成するステップと、データの第1の部分に前記第1の暗号鍵を含んだ前記第1の電子透かしを挿入するステップと、前記データの第2の部分を前記第1の暗号鍵で暗号化するステップと、を有することを特徴とする電子透かしに含めた暗号鍵を用いた暗号化方法をコンピュータに実行させるためのコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項56】 請求項55に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、前記暗号化方法は、第2の暗号鍵を含んだ第2の電子透かしを生成するステップと、前記第2の部分が前記第1の暗号鍵で暗号化される前に、前記第2の部分に前記第2の電子透かしを挿入するステップと、前記データの第3の部分を前記第2の暗号鍵で暗号化するステップと、

を更に有することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項57】 請求項55に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、

前記暗号化方法は、

第 n (n は1より大きい整数)の暗号鍵を含んだ第 n の電子透かしを生成するステップと、

10 第 n の部分が前記暗号化手段により第 $(n-1)$ の暗号鍵で暗号化される前に、前記第 n の部分に前記第 n の電子透かしを挿入するステップと、

前記データの第 $(n+1)$ の部分を前記第 n の暗号鍵で暗号化するステップと、

を更に有することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項58】 請求項55に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、

前記暗号化方法は、

20 前記データを圧縮するステップを更に備えることを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項59】 請求項58に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、前記暗号化方法は、前記データを暗号化する前に、前記データを圧縮することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

30 【請求項60】 請求項55に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、前記データは画像データ、音声データ及び文字データの少なくとも1つを含むことを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項61】 請求項55に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、

前記暗号化方法は、

前記第1の部分を媒体に出力するステップと、

40 前記第2の部分を前記媒体と同一の媒体に出力するステップと、

を更に有することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項62】 請求項55に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、

前記暗号化方法は、

前記第1の部分を媒体に出力するステップと、

50 前記第2の部分を前記媒体と異なった媒体に出力するステップと、

を更に有することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 63】 請求項 55 に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、前記第 1 の部分はコマーシャルを含むことを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 64】 データの第 1 の部分より第 1 の電子透かしを検出するステップと、
前記第 1 の電子透かしより第 1 の暗号鍵を抽出するステップと、
前記データの第 2 の部分を前記第 1 の暗号鍵で暗号解読するステップと、
を有することを特徴とする電子透かしに含めた暗号鍵を用いた復号化方法をコンピュータに実行させるためのコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 65】 請求項 64 に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、
前記暗号化方法は、
前記第 1 の暗号鍵で暗号解読された前記第 2 の部分より第 2 の電子透かしを検出するステップと、
前記第 2 の電子透かしより第 2 の暗号鍵を抽出するステップと、
前記データの第 3 の部分を前記第 2 の暗号鍵で暗号解読するステップと、
を更に有することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 66】 請求項 64 に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、
前記暗号化方法は、
第 $(n-1)$ (n は 1 より大きい整数) の暗号鍵で暗号解読された第 n の部分より第 n の電子透かしを検出するステップと、
前記第 n の電子透かしより第 n の暗号鍵を抽出するステップと、
前記データの第 $(n+1)$ の部分を前記第 n の暗号鍵で暗号解読するステップと、
を更に有することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 67】 請求項 64 に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、
前記暗号化方法は、
前記データを伸長するステップを更に有することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 68】 請求項 67 に記載のコンピュータプロ

グラムを記録したコンピュータ読み取り可能な記録媒体において、前記暗号化方法は、前記データが暗号解読された後に、前記データを伸長することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 69】 請求項 64 に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、前記データは画像データ、音声データ及び文字データの少なくとも 1 つを含むことを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 70】 請求項 64 に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、
前記暗号化方法は、
前記第 1 の部分を媒体から入力するステップと、
前記第 2 の部分を前記媒体と同一の媒体から入力するステップと、
を更に有することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 71】 請求項 64 に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、
前記暗号化方法は、
前記第 1 の部分を媒体から入力するステップと、
前記第 2 の部分を前記媒体と異なった媒体から入力するステップと、
を更に有することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 72】 請求項 64 に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、前記第 1 の部分はコマーシャルを含むことを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 73】 第 1 の暗号鍵を含んだ第 1 の電子透かしが挿入された第 1 の部分と、
前記第 1 の暗号鍵により暗号化された第 2 の部分と、
を有するデータが記録されたコンピュータ読み取り可能な記録媒体。

【請求項 74】 請求項 73 に記載のコンピュータ読み取り可能な記録媒体において、
前記第 2 の部分には、第 2 の暗号鍵を含んだ第 2 の電子透かしが挿入され、
前記データは、前記第 2 の暗号鍵により暗号化された第 3 の部分を有することを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項 75】 請求項 73 に記載のコンピュータ読み取り可能な記録媒体において、
前記第 n (n は 1 より大きい整数) の部分には、第 n の暗号鍵を含んだ第 n の電子透かしが挿入され、

前記データは、前記第 n の暗号鍵により暗号化された第 $(n+1)$ の部分を含むことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタルデータに電子透かしを挿入する方法及び装置並びにデジタルデータから電子透かしを検出する方法及び装置に関し、特に、デジタル画像データに電子透かしを挿入する方法及び装置並びにデジタル画像データから電子透かしを検出する方法及び装置に関する。

【0002】また、本発明はデジタルデータを暗号化する方法及び装置並びに暗号化されたデジタルデータを復号する方法及び装置に関し、特に、デジタル画像データを暗号化する方法及び装置並びに暗号化されたデジタル画像データを復号する方法及び装置に関する。

【0003】

【従来の技術】近年、画像データや音声データは、デジタル化されてから蓄積、伝送、配布等がされるようになってきた。一方、デジタル化に伴うデータの違法な複製が大きな問題となっている。電子透かしデータの挿入・検出技術は、そのような違法な複製を防止する技術として注目を浴びており、実現化に向けて検討が進んでいる。また、電子透かしデータとは別にデータやプログラム等の改竄を防ぐ技術として暗号化方式がある。これは、データやプログラム自体をある暗号キーにより暗号化し、その暗号キーがなければそのデータやプログラムがデータやプログラムとして成り立たないようにする技術である。

【0004】

【発明が解決しようとする課題】しかし、暗号化技術は、一度その暗号キーを解読されてしまうと、暗号化したデータも簡単にアクセスできてしまうと言う弱点があり、DVD(Digital Versatile Disk)に施されているCSS(Contents Scrambling System)のように、同一の暗号鍵(単一の暗号鍵又は1組の暗号鍵)で全てのDVDコンテンツを暗号化した場合、その暗号鍵を解読されると、全てのDVDコンテンツの暗号を解いて、不正にコピー出来てしまうということになる。

【0005】そこで、各コンテンツをコンテンツ毎の暗号鍵を用いて暗号化することによりCSSの問題点を解決できる。しかし、暗号鍵をコンテンツとは別のルートでDVDの購買者に送付すると、購買者はコンテンツ毎に異なった暗号鍵を再生機又は再生ソフトに設定しなければならず、購買者の操作が煩わしい。また、暗号鍵をMPEG(Moving Picture Experts Group)データの特定の領域に挿入すると、不正者が容易にMPEGデータから暗号鍵を抜き取り、抜き取った暗号鍵により暗号化されていないMPEGデータを取り出し、暗号化されていないMPEGデータを複製することが可能となってしまう

う。

【0006】特開平11-317859号公報に記載の技術は、電子透かしを画像データに挿入すると共に、電子透かしをスクランブルのための座標変換データの一部として使用して、画像ブロック単位で画像をスクランブルすることにより、再生側で、画像データに挿入された電子透かしと同一の電子透かしを用意している場合に限り、スクランブルを解除できるようにしたものである。しかし、この技術では、画像データの暗号化が行われておらず、画像ブロック単位でスクランブルが行われているだけであるので、スクランブルを解かなくても、どのフレームからも電子透かしを検出することができ、電子透かしを隠蔽することが全く出来ない。また、画像データを圧縮しようとした際、画像ブロック単位でスクランブルが行われているので、空間の連続性が無くなり、画像ブロックの動きベクトルを検出できず、動き補償フレーム間予測符号化を用いることが出来なくなってしまう。従って、高能率に圧縮することが出来なくなってしまう。

【0007】そこで、本発明では電子透かし技術と、暗号化技術のそれぞれの特徴を活かし、よりセキュアなデジタルコンテンツの再生制限をすることを可能とする、電子透かしに含めた暗号鍵を用いた暗号化装置及びその方法並びに電子透かしに含めた暗号鍵を用いた復号化装置及びその方法を提供することを目的とする。

【0008】

【課題を解決するための手段】本発明の第1の観点によれば、第1の暗号鍵を含んだ第1の電子透かしを生成する生成手段と、データの第1の部分に前記第1の暗号鍵を含んだ前記第1の電子透かしを挿入する電子透かし挿入手段と、前記データの第2の部分を前記第1の暗号鍵で暗号化する暗号化手段と、を備えることを特徴とする電子透かしに含めた暗号鍵を用いた暗号化装置が提供される。

【0009】上記の暗号化装置において、前記電子透かし生成手段は、第2の暗号鍵を含んだ第2の電子透かしを生成し、前記電子透かし挿入手段は、前記第2の部分が前記暗号化手段により前記第1の暗号鍵で暗号化される前に、前記第2の部分に前記第2の電子透かしを挿入し、前記暗号化手段は、前記データの第3の部分を前記第2の暗号鍵で暗号化してもよい。

【0010】上記の暗号化装置において、前記電子透かし生成手段は、第 n (n は1より大きい整数)の暗号鍵を含んだ第 n の電子透かしを生成し、前記電子透かし挿入手段は、第 n の部分が前記暗号化手段により第 $(n-1)$ の暗号鍵で暗号化される前に、前記第 n の部分に前記第 n の電子透かしを挿入し、前記暗号化手段は、前記データの第 $(n+1)$ の部分を前記第 n の暗号鍵で暗号化してもよい。

【0011】上記の暗号化装置は、前記データを圧縮す

る圧縮手段を更に備えていてもよい。

【0012】上記の暗号化装置において、前記圧縮手段は、前記データを暗号化する前に、前記データを圧縮してもよい。

【0013】上記の暗号化装置において、前記データは画像データ、音声データ及び文字データの少なくとも1つを含んでいてもよい。

【0014】上記の暗号化装置において、前記第1の部分と前記第2の部分は同一の媒体に出力されてもよい。

【0015】上記の暗号化装置において、前記第2の部分10は前記第1の部分と異なった媒体に出力されてもよい。

【0016】上記の暗号化装置において、前記第1の部分はコマーシャルを含んでいてもよい。

【0017】本発明の第2の観点によれば、データの第1の部分より第1の電子透かしを検出する電子透かし検出手段と、前記第1の電子透かしより第1の暗号鍵を抽出する暗号鍵抽出手段と、前記データの第2の部分を前記第1の暗号鍵で暗号解読する暗号解読手段と、を備えることを特徴とする電子透かしに含めた暗号鍵を用いた20 復号化装置が提供される。

【0018】上記の復号化装置において、前記電子透かし検出手段は、前記暗号解読手段により前記第1の暗号鍵で暗号解読された前記第2の部分より第2の電子透かしを検出し、前記暗号鍵抽出手段は、前記第2の電子透かしより第2の暗号鍵を抽出し、前記暗号解読手段は、前記データの第3の部分を前記第2の暗号鍵で暗号解読してもよい。

【0019】上記の復号化装置において、前記電子透かし検出手段は、前記暗号解読手段により第(n-1)30 (nは1より大きい整数)の暗号鍵で暗号解読された第nの部分より第nの電子透かしを検出し、前記暗号鍵抽出手段は、前記第nの電子透かしより第nの暗号鍵を抽出し、前記暗号解読手段は、前記データの第(n+1)の部分の前記第nの暗号鍵で暗号解読してもよい。

【0020】上記の復号化装置は、前記データを伸長する伸長手段を更に備えていてもよい。

【0021】上記の復号化装置において、前記伸長手段は、前記データが暗号解読された後に、前記データを伸長してもよい。

【0022】上記の復号化装置において、前記データは画像データ、音声データ及び文字データの少なくとも1つを含んでいてもよい。

【0023】上記の復号化装置において、前記第1の部分と前記第2の部分は同一の媒体から入力されてもよい。

【0024】上記の復号化装置において、前記第2の部分は前記第1の部分と異なった媒体から入力されてもよい。

【0025】上記の復号化装置において、前記第1の部50

分はコマーシャルを含んでいてもよい。

【0026】

【発明の実施の形態】以下、図面を参照して本発明の実施形態について詳細に説明する。

【0027】[実施形態1]図1は、実施形態1による音声画像データ符号化装置及びその周辺部の構成を示すブロック図である。

【0028】図1を参照すると、101は、音声を原音声データに変換するマイク、102は、画像を原画像データに変換するカメラ、103は、原音声データ及び原画像データを記憶している記憶装置、104は、マイク101からの原音声データ又は記憶装置からの原音声データを選択するスイッチ、105は、カメラ102からの原画像データ又は記憶装置103からの原画像データを選択し、原画像データ181を出力するスイッチである。

【0029】106は、世代管理情報ビット及び暗号鍵を記憶する記憶装置、107は、世代管理情報ビット及び暗号鍵を基にこれらを含む電子透かしを生成する電子透かし生成器、108は、電子透かし生成器107が生成した電子透かし185をスイッチ105からの原画像データに挿入して、電子透かし挿入済画像データ182を生成する電子透かし挿入器である。

【0030】109は、スイッチ104からの原音声データ及び電子透かし挿入器108からの電子透かし挿入済画像データを圧縮して非暗号化MPEGデータ183を生成するMPEGエンコーダ、110は、MPEGエンコーダ109からの非暗号化MPEGデータを記憶装置106からの暗号鍵により暗号化して暗号化されたMPEGデータを生成する暗号化器、111は、MPEGエンコーダ109からの非暗号化MPEGデータ又は暗号化器110からの暗号化されたMPEGデータを選択して一部が暗号化されたMPEGデータ184を出力するスイッチである。

【0031】なお、暗号化器110の行う暗号化は、例えば、DES(Data Encryption Standard)によるものであり、従って、暗号鍵は共通鍵である。

【0032】112は、各時点で暗号化を行うか否かの制御を行う暗号化／非暗号化制御部であり、制御信号を電子透かし生成器107、MPEGエンコーダ109、スイッチ111に出力する。

【0033】スイッチ111から出力される一部が暗号化されたMPEGデータは、記憶装置113に記憶され、DVD114に記録され、送信装置115から送信され、又は、ネットワーク116に送出される。送信装置115は、受信装置と対をなす送信装置のみならず放送局の放送用の送信装置も含む。

【0034】図2は、図1に示す電子透かし挿入器108の構成を示すブロック図である。

【0035】図2を参照すると、電子透かし挿入器10

8は、離散コサイン変換器121、電子透かしデータ保持部122、挿入部123、逆離散コサイン変換器124を備える。

【0036】離散コサイン変換器121は、空間領域の原画像データ $x(j)$ に対して、例えば8画素×8画素の2次元の離散コサイン変換を行い、周波数領域の係数 $f(i)$ を出力する。ここで、 j は、2次元から1次元に並べられた後の画素の番号を表し、 i は、2次元から1次元に並べられた後の係数の番号を表す。

【0037】電子透かしデータ保持部122は、電子透かしデータ

$w(1)$ 、 $w(2)$ 、 \dots 、 $w(n)$

を保持する。なお、電子透かしデータは平均0、分散1の正規分布に従う。

【0038】挿入部123は、以下のことを行う。すなわち、係数 $f(i)$ と電子透かしデータ $w(i)$ を基に、電子透かし挿入後の係数 $F(i)$ を、

$$F(i) = f(i) + \alpha \times \text{avg}(f(i)) \times w(i)$$

の計算式により各 i について計算する。ここで、 α はスケール要素であり、 $\text{avg}(f(i))$ は $f(i)$ の近傍3点の絶対値の平均を取った部分平均である。そして、 $F(i)$ を出力する。

【0039】逆離散コサイン変換器124は、電子透かし挿入後の係数 $F(i)$ に対して、逆離散コサイン変換を行い、空間領域の電子透かし挿入済画像データ $X(j)$ を出力する。

【0040】図3は、実施形態1による音声画像データ復号化装置及びその周辺部の構成を示すブロック図である。

【0041】図3を参照すると、141は、送信装置114から送信されてきた一部が暗号化されたMPEGデータを受信する受信装置である。受信装置141は、送信装置と対をなす受信装置のみならず、放送局から送信されてきた放送を受信する受信装置も含む。

【0042】142は、記憶装置113、DVD114、受信装置141及びネットワーク116のうちの何れかからの一部が暗号化されたMPEGデータを選択するスイッチである。

【0043】143は、一部が暗号化されたMPEGデータを入力し、各時点でそれが暗号化されているかいないかを検出する暗号化期間／非暗号化期間検出部であり、144は、一部が暗号化されたMPEGデータを入力し、暗号鍵抽出部154が電子透かしから抽出した暗号鍵を使用してその暗号を復号する暗号解読器、145は、暗号化／非暗号化検出部143からの暗号化期間／非暗号化期間検出信号に基づき、非暗号化期間では一部が暗号化されたMPEGデータを選択し、暗号化期間では暗号解読器144からの非暗号化MPEGデータを選択するスイッチである。なお、スイッチ145が非暗号

化期間で一部が暗号化されたMPEGデータを選択するときには、一部が暗号化されたMPEGデータは暗号化されていない。

【0044】146は、非暗号化MPEGデータを入力し、これを圧縮音声データと電子透かし挿入済圧縮画像データに分離して、これらを出力する画像／音声分離器、147は、圧縮音声データから音声データを復元する音声デコーダ、148は、復元音声データを増幅してスピーカ駆動信号を生成する音声増幅器、149はスピーカ駆動信号を基に音声を出力するスピーカである。

【0045】150は、電子透かし挿入済圧縮画像データから電子透かし挿入済復元画像データを復元する画像デコーダ、151は、電子透かし挿入済復元画像データを基にディスプレイ駆動信号を生成するディスプレイ駆動装置151、152は、ディスプレイ駆動信号を基に画像を表示するディスプレイである。

【0046】153は、電子透かし挿入済復元画像データから電子透かしを検出して、電子透かしを暗号解読器144に出力する電子透かし検出部、154は、電子透かしから暗号鍵を抽出し、暗号鍵を出力する暗号鍵抽出部、155は、電子透かしから世代管理情報ビットを抽出し、世代管理情報ビットを出力する世代管理情報ビット抽出部である。

【0047】世代管理情報ビットは、2ビットで表され、その値により、コピー・フリー(copy free)、コピー・ワンス(copy once)又はコピー禁止(inhibit)を示し、コピーマーク、メディアの種類の情報との組み合わせにより再生禁止、コピー禁止のために用いられるが、本発明の範囲外であるので、その説明は省略する。

30 【0048】図4は、図3に示す電子透かし検出器153の構成を示すブロック図である。

【0049】図4を参照すると、電子透かし検出器153は、離散コサイン変換器161、電子透かしデータ候補保持部162、検出部163を備える。

【0050】離散コサイン変換器161は、空間領域の電子透かし挿入済画像データ $X(j)$ に対して離散コサイン変換を行い、電子透かし挿入後の係数 $F(i)$ を出力する。

【0051】電子透かしデータ候補保持部162は、複数の電子透かしデータ候補を保持する。

【0052】検出部163は、電子透かし挿入後の係数 $F(i)$ を基に、電子透かしデータ $W(i)$ を、 $W(i) = F(i) / \text{avg}(F(i))$ の計算式により計算し、1フレーム分の $W(i)$ の総和 $WF(i)$ を各 i について計算する。

【0053】次に、検出部163は、電子透かし候補 $w(i)$ と $WF(i)$ との統計的類似度 C をベクトルの内積を利用して、

$$C = WF \times w / (WF D \times w D)$$

の計算式により計算する。ここで、

WF = (WF (1)、WF (2)、・・・、WF (n))、
w = (w (1)、w (2)、・・・、w (n))、
WFD = ベクトル WF の絶対値、
wD = ベクトル w の絶対値

である。統計的類似度 C がある特定の値以上である場合には、該当電子透かしデータが埋め込まれていると判定する。

【0054】図5は、実施形態1による音声画像データ符号化装置の各部が出力する信号を示す図であり、スイッチ105が出力する原画像データ181、電子透かし挿入器108が出力する電子透かし挿入済画像データ182、MPEGエンコーダ109が出力する非暗号化MPEGデータ183、スイッチ184が出力する一部が暗号化されたMPEGデータ194を示す。

【0055】図5を参照すると、電子透かし挿入済画像データ182に挿入される電子透かし185は、8ビットより構成され、符号185-1で示すように、非暗号化期間では、2ビットの世代管理情報ビットと6ビットの暗号鍵より構成され、符号185-2で示すように、暗号化期間では2ビットの世代管理情報ビットと任意の値を取る6ビットより構成される。なお、図5の例では、世代管理情報ビットは、"11(binary)"の値を取り、これは、コピー禁止を示す。

【0056】1つの電子透かしには、6ビットの暗号鍵しか入れられないが、暗号鍵を分割して、複数の電子透かしに分散して挿入することにより、6ビットよりもビット数が多い暗号鍵を電子透かしとして画像データに挿入することができる。例えば、15フレームに1つの電子透かしを挿入することができるので、NTSC方式であれば、約2秒間に24ビットの暗号鍵を画像データに挿入することができる。但し、電子透かしを挿入した後の画質を考慮して、2秒よりも長い時間に24ビットの暗号鍵を挿入するようにしても良い。

【0057】一部が暗号化されたMPEGデータ184は、符号184-1で示すように、非暗号化期間では、暗号化されず、符号184-2で示すように、暗号化期間では、暗号化される。

【0058】なお、暗号化期間及び非暗号化期間のMPEGデータへの割当は、ファイル毎に行っても良いし、シーケンス毎に行っても良い。また、MPEGデータのプライベート・パケットに暗号化期間/非暗号化期間を示すフラグを挿入したり、非暗号化期間を固定時間とすれば、暗号化期間及び非暗号化期間のMPEGデータへの割当をファイル毎又はシーケンス毎に行わなくても良い。

【0059】図6は、実施形態1による音声画像データ符号化装置の主要な部分の動作を示すタイミング図である。

【0060】図6を参照すると、非暗号化期間では、電

子透かし生成器107は、暗号鍵を含む電子透かし185-1を生成し、電子透かし挿入器108は、原画像データに電子透かし185-1を挿入し、MPEGエンコーダ109は、電子透かし挿入済画像データに対しMPEGエンコードを行い、スイッチ111は、MPEGエンコーダ109からの非暗号化MPEGデータ183を選択する。なお、暗号化器110は、非暗号化期間では、非暗号化MPEGデータの暗号化を行わない。

【0061】暗号化期間では、電子透かし生成器107は、暗号鍵を含まない電子透かし185-2を生成し、電子透かし挿入器108は、原画像データに電子透かし185-2を挿入し、MPEGエンコーダ109は、電子透かし挿入済画像データに対しMPEGエンコードを行い、暗号化器110は非暗号化MPEGデータを非暗号化期間で電子透かしに含めた暗号鍵で暗号化し、スイッチ111は、暗号化されたMPEGデータ185を選択する。

【0062】図7は、実施形態1による音声画像データ復号化装置の主要な部分の動作を示すタイミング図である。

【0063】図7を参照すると、非暗号化期間では、暗号化期間/非暗号化期間検出部143は、一部が暗号化されたMPEGデータが暗号化されているか否かを検出する。検出の方法は、ファイル毎に暗号化期間及び非暗号化期間がMPEGデータへ割当てられているか、シーケンス毎に暗号化期間及び非暗号化期間がMPEGデータへ割当てられているか、MPEGデータのプライベート・パケットに暗号化期間/非暗号化期間を示すフラグを挿入されているか、又は、非暗号化期間を固定時間とされているかにより異なる。

【0064】また、非暗号化期間では、画像/音声分離器146は、非暗号化MPEGデータを圧縮音声データと電子透かし挿入済圧縮画像データに分離し、音声デコーダ147は、圧縮音声データより音声データを復元し、画像デコーダ150は、電子透かし挿入済圧縮画像データより電子透かし挿入済画像データを復元し、電子透かし検出部153は、電子透かし挿入済画像データより世代管理情報ビットと暗号鍵を含む電子透かしを検出し、暗号鍵抽出部154は、電子透かしより暗号鍵を抽出し、世代管理情報ビット抽出部155は、電子透かしより世代管理情報ビットを抽出し、スイッチ145は、暗号解読器144が入力する一部が暗号化されたMPEGデータと同一のデータを選択する。非暗号化期間では、一部が暗号化されたMPEGデータは暗号化されていない。

【0065】なお、非暗号化期間では暗号解読器144は、暗号の解読を行わない。

【0066】暗号化期間では、暗号化期間/非暗号化期間検出部143は、一部が暗号化されたMPEGデータが暗号化されているか否かを検出し、暗号解読器144

は、暗号化されたMP E Gデータの暗号を非暗号化期間で暗号鍵抽出部154が電子透かしより抽出した暗号鍵を用いて解読し、画像／音声分離器146は、非暗号化MP E Gデータを圧縮音声データと電子透かし挿入済圧縮画像データに分離し、音声デコーダ147は、圧縮音声データより音声データを復元し、画像デコーダ150は、電子透かし挿入済圧縮画像データより電子透かし挿入済画像データを復元し、電子透かし検出部153は、電子透かし挿入済画像データより世代管理情報ビットを含む電子透かしを検出し、世代管理情報ビット抽出部155は、電子透かしより世代管理情報ビットを抽出し、スイッチ145は、暗号解読器144が出力する非暗号化MP E Gデータを選択する。

【0067】なお、暗号化期間では、暗号鍵抽出部154は、電子透かしより暗号鍵を抽出しない。

【0068】実施形態1によれば、以下の効果が奏される。

【0069】1つのコンテンツの暗号鍵が見破られても、その暗号鍵により他のコンテンツの暗号を解読することが出来ないで、コンテンツ制作者の著作権を厚く保護することができる。また、1つのコンテンツを複数の部分に分割した上で実施形態1を適用した場合には、1つの部分の暗号鍵が見破られても、その暗号鍵により他の部分の暗号鍵を解読することが出来ないで、コンテンツ制作者の著作権を厚く保護することができる。

【0070】暗号鍵がコンテンツ内に含まれているので、視聴者が暗号鍵をコンテンツと別ルートで入手し、再生機に設定する必要がなくなる。

【0071】暗号鍵がそのままの形でMP E Gデータに挿入されていないので、暗号鍵をMP E Gデータから抜き出すことが困難になる。特に、再生装置を暗号鍵抽出部が出力する暗号鍵を外部からアクセスすることを防止できるような構造とすることにより、不正者が暗号鍵を抜き出すことが不可能となる。

【0072】再生装置は、電子透かし検出器を有さなければ、音声及び画像を再生することが出来ないで、電子透かし検出器を有しない海賊版の再生装置で、音声及び画像を再生することが出来ない。

【0073】暗号鍵を含む電子透かしが挿入されている画像データを再生しなければ、暗号化されている画像データの暗号を復号することが出来ないで、例えば、コマーシャルに暗号鍵を含む電子透かしを挿入することにより、視聴者が必ずコマーシャルを視聴することになり、従って、コンテンツ制作者はスポンサーからの収益源を確保することが出来る。

【0074】〔実施形態2〕実施形態2は、MP E Gデータのうちの第1の暗号鍵により暗号化された第1の暗号化期間の電子透かしに第2の暗号鍵を含ませ、その第2の暗号鍵によりMP E Gデータのうちの他の部分を暗号化し、このような暗号化の連鎖を繰り返すものであ

る。すなわち、暗号化期間を複数の暗号化期間に分割し、それぞれの暗号化期間のMP E Gデータを他の暗号化期間の電子透かしに含まれている暗号鍵により暗号化するものである。

【0075】実施形態2による音声画像データ符号化装置の構成は、図1に示す実施形態1による音声画像データ符号化装置と同一であるので、その説明は省略する。また、実施形態2による音声画像データ復号化装置の構成は、図3に示す実施形態1による音声画像データ復号化装置と同一であるので、その説明も省略する。

【0076】図8は、実施形態2による音声画像データ符号化装置の各部が出力する信号を示す図であり、スイッチ105が出力する原画像データ181、電子透かし挿入器108が出力する電子透かし挿入済画像データ182、MP E Gエンコーダ109が出力する非暗号化MP E Gデータ183、スイッチ184が出力する一部が暗号化されたMP E Gデータ194を示す。

【0077】図8を参照すると、電子透かし挿入済画像データ182に挿入される電子透かし185は、8ビットより構成され、符号185-3で示すように、非暗号化期間では、2ビットの世代管理情報ビットと6ビットの第1の暗号鍵より構成され、符号185-4で示すように、第1の暗号鍵による暗号化期間では、2ビットの世代管理情報ビットと6ビットの第2の暗号鍵より構成され、符号185-5で示すように、第2の暗号鍵による暗号化期間では、2ビットの世代管理情報ビットと6ビットの第3の暗号鍵より構成され、符号185-6で示すように、第3の暗号鍵による暗号化期間では2ビットの世代管理情報ビットと任意の値を取る6ビットより構成される。なお、図8の例では、図5の例と同様に、世代管理情報ビットは、“11(binary)”の値を取り、これは、コピー禁止を示す。

【0078】一部が暗号化されたMP E Gデータ184は、符号184-3で示すように、非暗号化期間では、暗号化されず、符号184-4で示すように、第1の暗号鍵による暗号化期間（第1の暗号化期間）では、第1の暗号鍵により暗号化され、符号184-5で示すように、第2の暗号鍵による暗号化期間（第2の暗号化期間）では、第2の暗号鍵により暗号化され、符号184-6で示すように、第3の暗号鍵による暗号化期間（第3の暗号化期間）では、第3の暗号鍵により暗号化される。

【0079】なお、第1乃至第3の暗号化期間及び非暗号化期間のMP E Gデータへの割当は、ファイル毎に行っても良いし、シーケンス毎に行っても良い。また、MP E Gデータのプライベート・バケットに第1乃至第3の暗号化期間／非暗号化期間を示すフラグを挿入したり、第1乃至第3の暗号化期間及び非暗号化期間を固定時間とすれば、第1乃至第3の暗号化期間及び非暗号化期間のMP E Gデータへの割当をファイル毎又はシーケ

10

20

30

40

50

ンス毎に行わなくても良い。

【0080】図9は、実施形態2による音声画像データ符号化装置の主要な部分の動作を示すタイミング図である。

【0081】図9を参照すると、非暗号化期間では、電子透かし生成器107は、第1の暗号鍵を含む電子透かし185-3を生成し、電子透かし挿入器108は、原画像データに電子透かし185-3を挿入し、MPEGエンコーダ109は、電子透かし挿入済画像データに対しMPEGエンコードを行い、スイッチ111は、MPEGエンコーダ109からの非暗号化MPEGデータ183を選択する。なお、暗号化器110は、非暗号化期間では、非暗号化MPEGデータの暗号化を行わない。

【0082】第1の暗号化期間では、電子透かし生成器107は、第2の暗号鍵を含む電子透かし185-4を生成し、電子透かし挿入器108は、原画像データに電子透かし185-4を挿入し、MPEGエンコーダ109は、電子透かし挿入済画像データに対しMPEGエンコードを行い、暗号化器110は非暗号化MPEGデータを非暗号化期間で電子透かしに含めた第1の暗号鍵で暗号化し、スイッチ111は、暗号化されたMPEGデータ185を選択する。

【0083】第2の暗号化期間では、電子透かし生成器107は、第3の暗号鍵を含む電子透かし185-5を生成し、電子透かし挿入器108は、原画像データに電子透かし185-5を挿入し、MPEGエンコーダ109は、電子透かし挿入済画像データに対しMPEGエンコードを行い、暗号化器110は非暗号化MPEGデータを第1の暗号鍵による暗号化期間で電子透かしに含めた第2の暗号鍵で暗号化し、スイッチ111は、暗号化されたMPEGデータ185を選択する。

【0084】第3の暗号化期間では、電子透かし生成器107は、暗号鍵を含まない電子透かし185-6を生成し、電子透かし挿入器108は、原画像データに電子透かし185-6を挿入し、MPEGエンコーダ109は、電子透かし挿入済画像データに対しMPEGエンコードを行い、暗号化器110は非暗号化MPEGデータを第2の暗号鍵による暗号化期間で電子透かしに含めた第3の暗号鍵で暗号化し、スイッチ111は、暗号化されたMPEGデータ185を選択する。

【0085】図10は、実施形態2による音声画像データ復号化装置の主要な部分の動作を示すタイミング図である。

【0086】図10を参照すると、非暗号化期間では、暗号化期間／非暗号化期間検出部143は、一部が暗号化されたMPEGデータが暗号化されているか否かを検出する。検出の方法は、実施形態1と同様である。

【0087】また、非暗号化期間では、画像／音声分離器146は、非暗号化MPEGデータを圧縮音声データと電子透かし挿入済圧縮画像データに分離し、音声デコ

ーダ147は、圧縮音声データより音声データを復元し、画像デコーダ150は、電子透かし挿入済圧縮画像データより電子透かし挿入済画像データを復元し、電子透かし検出部153は、電子透かし挿入済画像データより世代管理情報ビットと第1の暗号鍵を含む電子透かしを検出し、暗号鍵抽出部154は、電子透かしより第1の暗号鍵を抽出し、世代管理情報ビット抽出部155は、電子透かしより世代管理情報ビットを抽出し、スイッチ145は、暗号解読器144が入力する一部が暗号化されたMPEGデータと同一のデータを選択する。非暗号化期間では、一部が暗号化されたMPEGデータは暗号化されていない。

【0088】なお、非暗号化期間では暗号解読器144は、暗号の解読を行わない。

【0089】第1の暗号化期間では、暗号化期間／非暗号化期間検出部143は、一部が暗号化されたMPEGデータが暗号化されているか否かを検出し、暗号解読器144は、暗号化されたMPEGデータの暗号を非暗号化期間で暗号鍵抽出部154が電子透かしより抽出した第1の暗号鍵を用いて解読し、画像／音声分離器146は、非暗号化MPEGデータを圧縮音声データと電子透かし挿入済圧縮画像データに分離し、音声デコーダ147は、圧縮音声データより音声データを復元し、画像デコーダ150は、電子透かし挿入済圧縮画像データより電子透かし挿入済画像データを復元し、電子透かし検出部153は、電子透かし挿入済画像データより世代管理情報ビット及び第2の暗号鍵を含む電子透かしを検出し、暗号鍵抽出部154は、電子透かしより第2の暗号鍵を抽出し、世代管理情報ビット抽出部155は、電子透かしより世代管理情報ビットを抽出し、スイッチ145は、暗号解読器144が出力する非暗号化MPEGデータを選択する。

【0090】第2の暗号化期間では、暗号化期間／非暗号化期間検出部143は、一部が暗号化されたMPEGデータが暗号化されているか否かを検出し、暗号解読器144は、暗号化されたMPEGデータの暗号を第1の暗号化期間で暗号鍵抽出部154が電子透かしより抽出した第2の暗号鍵を用いて解読し、画像／音声分離器146は、非暗号化MPEGデータを圧縮音声データと電子透かし挿入済圧縮画像データに分離し、音声デコーダ147は、圧縮音声データより音声データを復元し、画像デコーダ150は、電子透かし挿入済圧縮画像データより電子透かし挿入済画像データを復元し、電子透かし検出部153は、電子透かし挿入済画像データより世代管理情報ビット及び第3の暗号鍵を含む電子透かしを検出し、暗号鍵抽出部154は、電子透かしより第3の暗号鍵を抽出し、世代管理情報ビット抽出部155は、電子透かしより世代管理情報ビットを抽出し、スイッチ145は、暗号解読器144が出力する非暗号化MPEGデータを選択する。

【0091】第3の暗号化期間では、暗号化期間／非暗号化期間検出部143は、一部が暗号化されたMPEGデータが暗号化されているか否かを検出し、暗号解読器144は、暗号化されたMPEGデータの暗号を第2の暗号化期間で暗号鍵抽出部154が電子透かしより抽出した第3の暗号鍵を用いて解読し、画像／音声分離器146は、非暗号化MPEGデータを圧縮音声データと電子透かし挿入済圧縮画像データに分離し、音声デコーダ147は、圧縮音声データより音声データを復元し、画像デコーダ150は、電子透かし挿入済圧縮画像データより電子透かし挿入済画像データを復元し、電子透かし検出部153は、電子透かし挿入済画像データより世代管理情報ビットを含む電子透かしを検出し、世代管理情報ビット抽出部155は、電子透かしより世代管理情報ビットを抽出し、スイッチ145は、暗号解読器144が出力する非暗号化MPEGデータを選択する。

【0092】なお、第3の暗号化期間では、暗号鍵抽出部154は、電子透かしより暗号鍵を抽出しない。

【0093】実施形態2によれば、実施形態1による効果に加え、以下の効果が奏される。

【0094】暗号化期間を複数の暗号化期間に分割し、それぞれの暗号化期間のMPEGデータを他の暗号化期間の電子透かしに含まれている暗号鍵により暗号化しているので、暗号化期間全体の暗号を解くための暗号鍵を解読する時間が分割数に比例して増大する。従って、電子透かし検出器を有しない不正者が不正に暗号鍵を解読しようとする意欲を失わせることができる。また、不正に暗号鍵を解読して音声画像を停止無しに連続して再生することを防止することができる。

【0095】〔実施形態3〕実施形態3を、その概念図である図11を参照して説明する。

【0096】非暗号化MPEGデータ201は、記憶装置203に記憶されており、コンピュータ206からの要求に従い、記憶装置202からWWWサーバ204、インターネット等のネットワークを通じてコンピュータ206に伝送される。コンピュータに伝送された非暗号化MPEGデータ201は、コンピュータの外部記憶装置等（不図示）に記憶される。WWWサーバ204からコンピュータ206への非暗号化MPEGデータ201の伝送には、TCP/IP(Transmission Control Protocol/Internet Protocol)上のFTP(file transfer protocol)等が用いられる。

【0097】暗号化MPEGデータ202は、DVD等の可搬の記録媒体207に記録される。

【0098】非暗号化MPEGデータ201は、暗号化MPEGデータに比べて、極めて小容量であり、これを記憶装置203からコンピュータ206に伝送する時間は、暗号化MPEGデータを伝送する場合に比べて、極めて短い。また、非暗号化MPEGデータ201には、暗号化MPEGデータ202の暗号を解読するための暗

号鍵が電子透かしの一部又は全部として挿入されている。更に、非暗号化MPEGデータの画像内容は、暗号化MPEGデータ202のコンテンツを示したり、その広告をしたりするものであることが好ましい。暗号化MPEGデータ202は、非暗号化MPEGデータ201に電子透かしの一部又は全部として含まれる暗号鍵により暗号化されている。

【0099】使用者は、暗号化MPEGデータ202のコンテンツを視聴しようとしたならば、コンピュータ206を操作することにより、記憶装置203に記憶されている非暗号化MPEGデータ201をコンピュータ206にダウンロードして記憶させ、また、コンテンツ製造者から流通経路、店舗を介して記録媒体207を入手して、コンピュータ206にローディングする。コンピュータ206により実現される音声画像データ復号装置は、使用者からの操作に従い、まず、非暗号化MPEGデータ201を再生し、この際に、電子透かしを検出し、検出された電子透かしから暗号鍵を抽出する。次に、コンピュータ206は、抽出された暗号鍵を用いて暗号を解読しながら暗号化MPEGデータから音声画像を再生する。

【0100】コンテンツ制作者は、コンピュータ206が非暗号化MPEGデータをダウンロードする際に、暗号化MPEGデータ202のコンテンツについて課金を行う。

【0101】なお、上記の実施形態3の説明では、音声画像データ復号装置はコンピュータにより実現されるとしたが、音声画像データ復号専用装置又は音声画像データ復号装置を兼ねた如何なる装置であっても良い。

【0102】また、上記の実施形態3の説明では、暗号化MPEGデータ202はDVD等の可搬な記録媒体に記録されているとしたが、暗号化MPEGデータ202が放送され、音声画像復号装置が暗号化MPEGデータ202を受信して、外部記憶装置に記憶してから、再生するようにしても良い。

【0103】実施形態3によれば、コンテンツをネットワークをダウンロードするための時間を短縮することができる。また、非暗号化MPEGデータ201をダウンロードするためのWWWサイトに広告を掲載することにより、コンテンツ制作者は、広告収入を得て、コンテンツの価格を下げる事が可能となる。

【0104】〔他の実施形態〕実施形態3では、非暗号化MPEGデータを通信によりコンテンツ事業者から消費者に配り、暗号化MPEGデータをパッケージの形態でコンテンツ事業者から消費者に配るとしたが、非暗号化MPEGデータ及び暗号化MPEGデータは、それぞれ、コンテンツ事業者から消費者に通信により配られても良いし、パッケージの形態で配られても良いし、放送の形態で配られても良い。

【0105】実施形態1乃至3では、画像データに電子

透かしを挿入するとしたが、音声データ、文字データに電子透かしを挿入しても良い。実施形態1乃至3では、画像データ及び音声データを暗号化するとしたが、画像データのみ又は音声データのみを暗号化しても良い。また、文字データを暗号化しても良い。例えば、画像データの第1の部分に暗号鍵を含む電子透かしを挿入し、画像データの第2の部分のみを暗号化しても良いし、音声データの第1の部分に暗号鍵を含む電子透かしを挿入し、音声データの第2の部分のみを暗号化しても良いし、文字データの第1の部分に暗号鍵を含む電子透かしを挿入し、文字データの第2の部分のみを暗号化しても良い。また、画像データの第1の部分に暗号鍵を含む電子透かしを挿入し、画像データの第2の部分、音声データ及び文字データを暗号化しても良いし、音声データの第1の部分に暗号鍵を含む電子透かしを挿入し、音声データの第2の部分、画像データ及び文字データを暗号化しても良いし、文字データの第1の部分に暗号鍵を含む電子透かしを挿入し、文字データの第2の部分、画像データ及び音声データを暗号化しても良い。

【0106】実施形態2において、1つの長編のコンテンツを複数のDVDに分割して収録し、1のDVDに収録されているMPEGデータを他のDVDに収録されているMPEGデータに挿入されている電子透かしに含まれる暗号鍵で暗号化するようにしてもよい。

【0107】図1に示す音声画像データ符号化装置及び図3に示す音声画像データ復号化装置は、それぞれ、必ずしもハードウェアにより実現されていなくても良い。すなわち、図1に示す音声画像データ符号化装置及び図3に示す音声画像データ復号化装置は、それぞれ、コンピュータを図1に示す音声画像データ符号化装置及び図3に示す音声画像データ復号化装置として機能させるためのプログラムをコンピュータが実行することによっても実現することができる。この場合、そのようなプログラムは、CD-ROM等の記録媒体に記録されていることもあり、コンピュータがネットワークを介して他のコンピュータからダウンロードする場合もある。

【0108】実施形態1乃至3では、非暗号化MPEGデータに電子透かしを挿入し、その電子透かしに暗号鍵を含め、その暗号鍵を用いて暗号化MPEGデータの暗号を解読するようにしたが、必ずしも、暗号化MPEGデータが暗号化されている必要はない。例えば、MPEGデータを非隠蔽MPEGデータと隠蔽MPEGデータに分割し、非隠蔽MPEGデータに電子透かしを挿入し、その電子透かしに隠蔽MPEGデータの隠蔽を外すための隠蔽解除鍵を含め、その隠蔽解除鍵を用いて隠蔽MPEGデータの隠蔽を外すようにしても良い。本発明では、このような隠蔽化も暗号化に含むものとし、隠蔽解除鍵も暗号鍵に含むものとする。

【0109】実施形態1乃至3では、音声画像圧縮方式としてMPEGデータを生成する方式を例に取り説明し

たが、他の方式であっても良い。また、音声画像の圧縮は省略しても良い。

【0110】

【発明の効果】以上説明したように、本発明によれば、以下の効果が奏される。

【0111】1つのコンテンツの暗号鍵が見破られても、その暗号鍵により他のコンテンツの暗号を解読することが出来ないで、コンテンツ制作者の著作権を厚く保護することができる。また、1つのコンテンツを複数の部分に分割した上で実施形態1を適用した場合には、1つの部分の暗号鍵が見破られても、その暗号鍵により他の部分の暗号鍵を解読することが出来ないで、コンテンツ制作者の著作権を厚く保護することができる。

【0112】暗号鍵がコンテンツ内に含まれているので、視聴者が暗号鍵をコンテンツと別ルートで入手し、再生機に設定する必要がなくなる。

【0113】暗号鍵がそのままの形でMPEGデータに挿入されていないので、暗号鍵をMPEGデータから抜き出すことが困難になる。特に、再生装置を暗号鍵抽出部が出力する暗号鍵を外部からアクセスすることを防止できるような構造とすることにより、不正者が暗号鍵を抜き出すことが不可能となる。

【0114】再生装置は、電子透かし検出器を有さなければ、音声及び画像を再生することが出来ないで、電子透かし検出器を有しない海賊版の再生装置で、音声及び画像を再生することが出来ない。

【0115】暗号鍵を含む電子透かしが挿入されている画像データを再生しなければ、暗号化されている画像データの暗号を復号することが出来ないで、例えば、コマーシャルに暗号鍵を含む電子透かしを挿入することにより、視聴者が必ずコマーシャルを視聴することになり、従って、コンテンツ制作者はスポンサーからの収益源を確保することが出来る。

【0116】暗号化期間を複数の暗号化期間に分割し、それぞれの暗号化期間のMPEGデータを他の暗号化期間の電子透かしに含まれている暗号鍵により暗号化しているので、暗号化期間全体の暗号を解くための暗号鍵を解読する時間が分割数に比例して増大する。従って、電子透かし検出器を有しない不正者が不正に暗号鍵を解読しようとする意欲を失わせることができる。また、不正に暗号鍵を解読して音声画像を停止無しに連続して再生することを防止することができる。

【図面の簡単な説明】

【図1】本発明の実施形態による音声画像データ符号化装置及びその周辺部の構成を示すブロック図である。

【図2】図1に示す電子透かし挿入器の一例の構成を示すブロック図である。

【図3】本発明の実施形態による音声画像データ復号化装置及びその周辺部の構成を示すブロック図である。

【図4】図3に示す電子透かし検出器の一例の構成を示

すブロック図である。

【図5】本発明の実施形態1による音声画像データ符号化装置の主要部が入出力するデータを示す図である。

【図6】本発明の実施形態1による音声画像データ符号化装置の主要部の動作を示すタイミング図である。

【図7】本発明の実施形態1による音声画像データ復号化装置の主要部の動作を示すタイミング図である。

【図8】本発明の実施形態2による音声画像データ符号化装置の主要部が入出力するデータを示す図である。

【図9】本発明の実施形態2による音声画像データ符号化装置の主要部の動作を示すタイミング図である。

【図10】本発明の実施形態2による音声画像データ復号化装置の主要部の動作を示すタイミング図である。

【図11】本発明の実施形態3を説明するための概念図である。

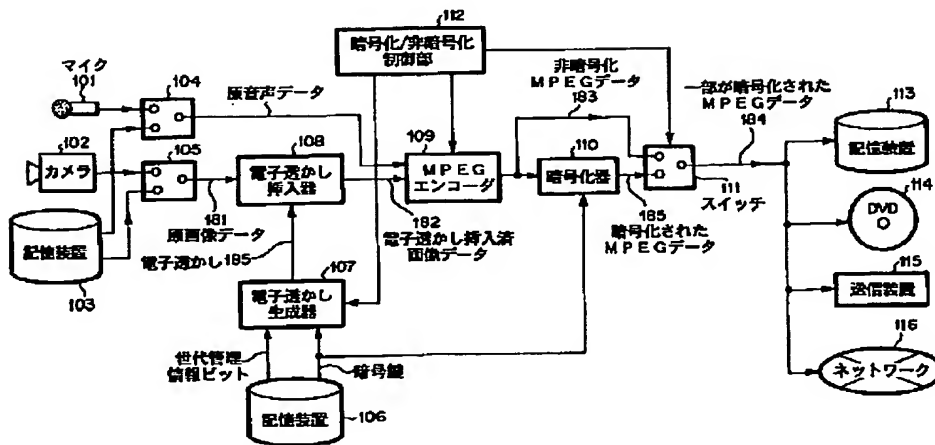
【符号の説明】

101 マイク
102 カメラ
103 記憶装置
104 スイッチ
105 スイッチ
106 記憶装置
107 電子透かし生成器
108 電子透かし挿入器
109 MPEGエンコーダ
110 暗号化器
111 スイッチ
112 暗号化/非暗号化制御部
113 記憶装置
114 DVD
115 送信装置
116 ネットワーク

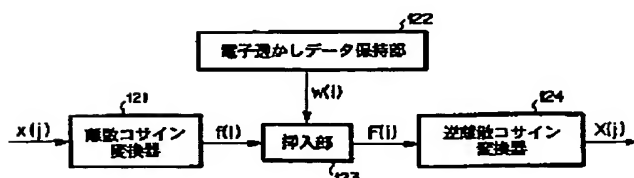
20

109 MPEGエンコーダ
110 暗号化器
111 スイッチ
112 暗号化/非暗号化制御部
113 記憶装置
114 DVD
115 送信装置
116 ネットワーク
141 受信装置
142 スイッチ
143 暗号化期間/非暗号化期間検出器
144 暗号解読器
145 スイッチ
146 画像/音声分離器
147 音声デコーダ
148 音声増幅器
149 スピーカ
150 画像デコーダ
151 ディスプレイ駆動装置
152 ディスプレイ
153 電子透かし検出器
154 暗号鍵抽出部
155 世代管理情報ビット抽出部

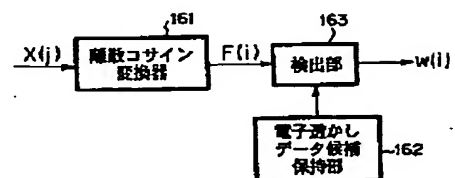
【図1】



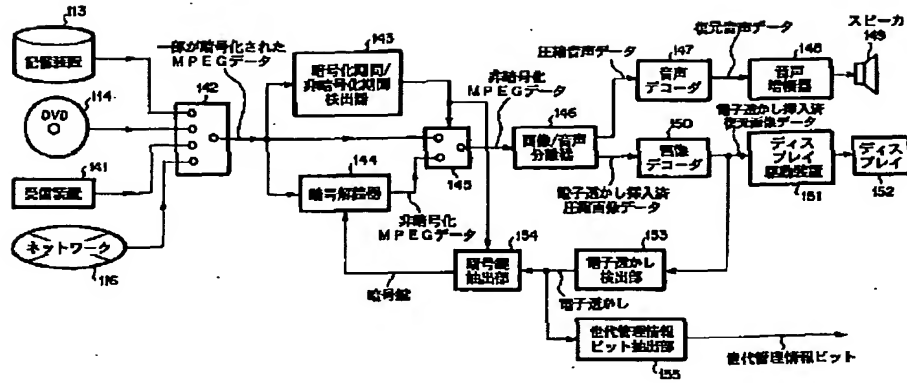
【図2】



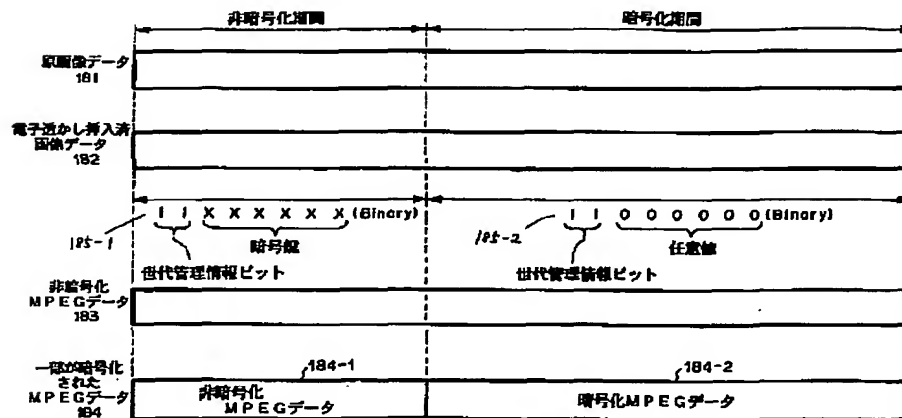
【図4】



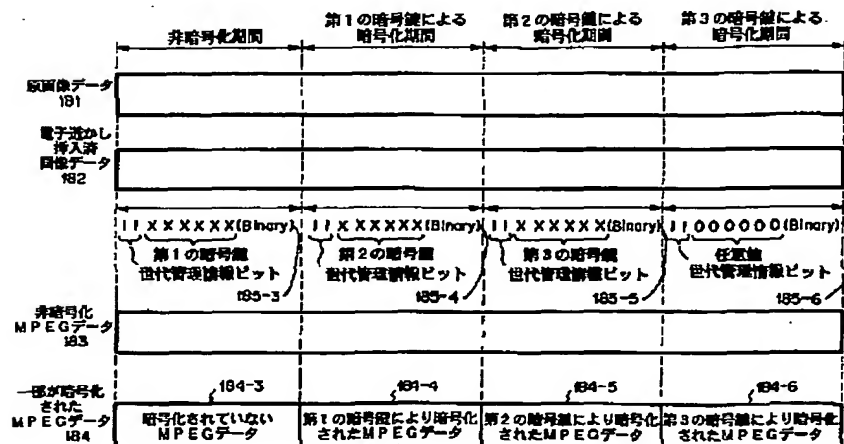
【図3】



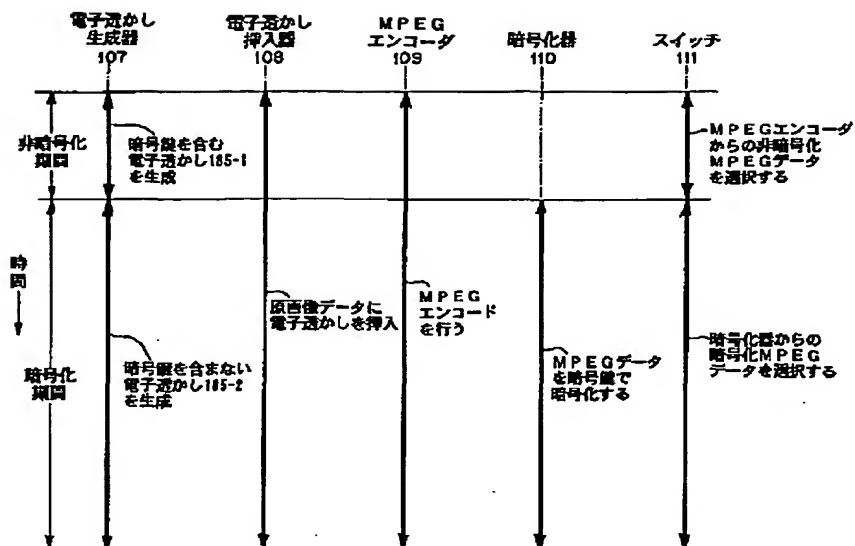
【図5】



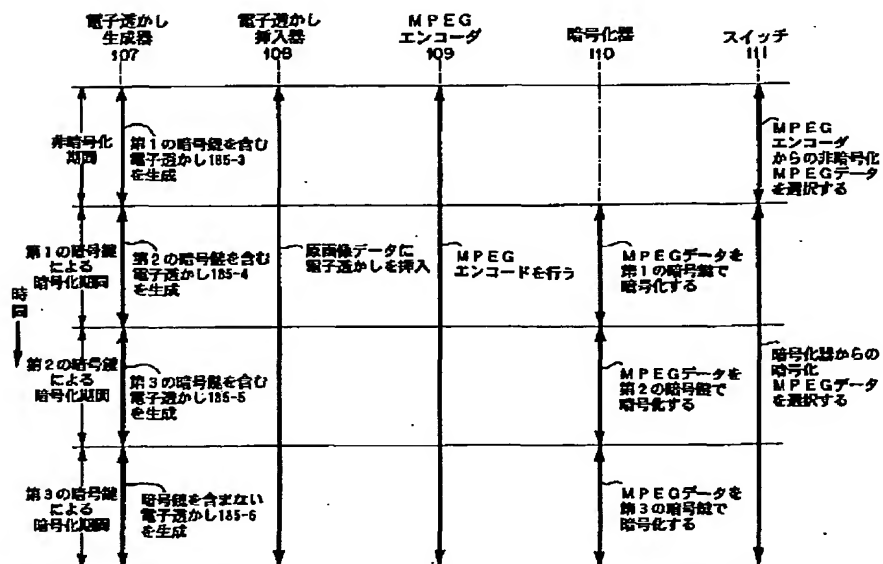
【図8】



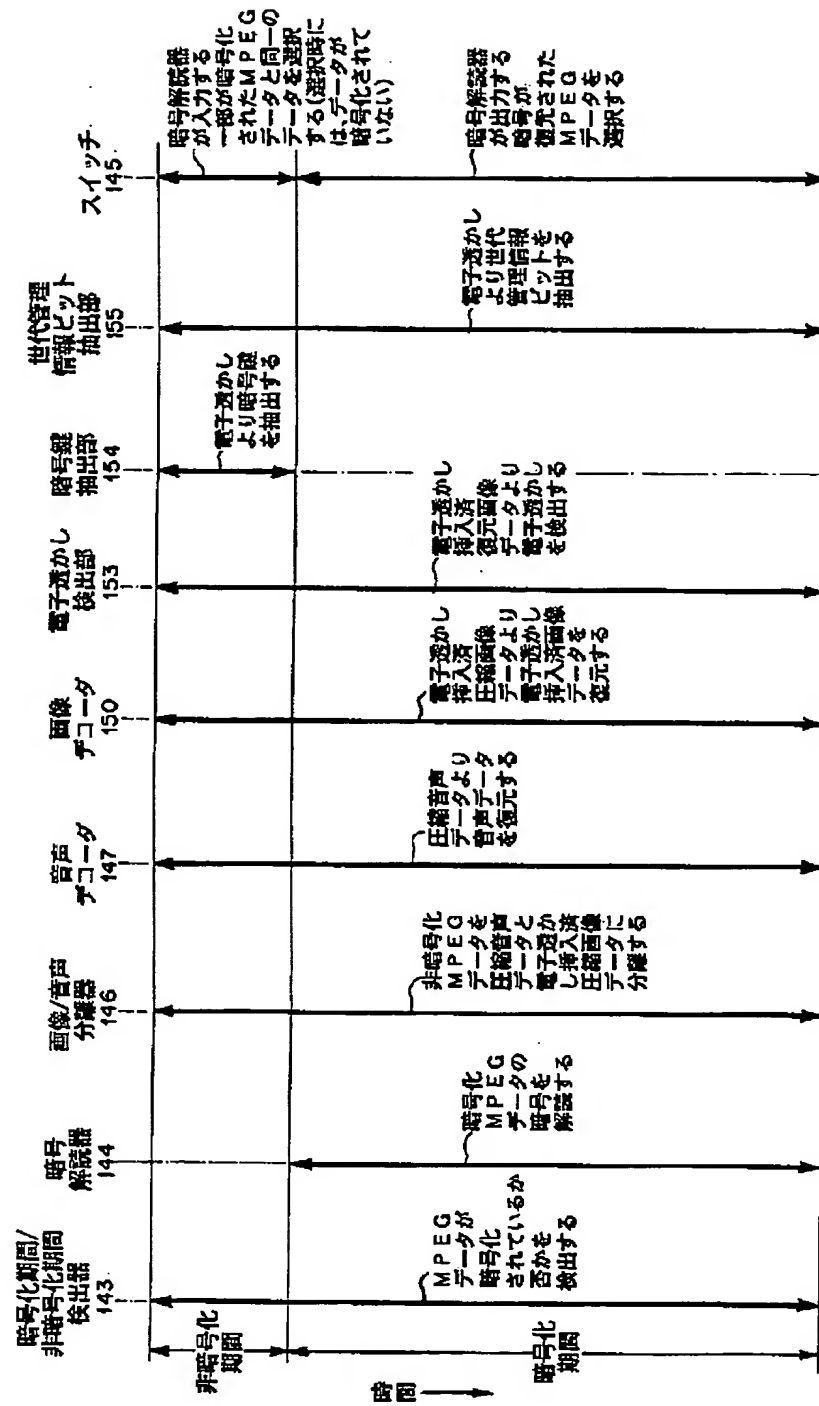
【図6】



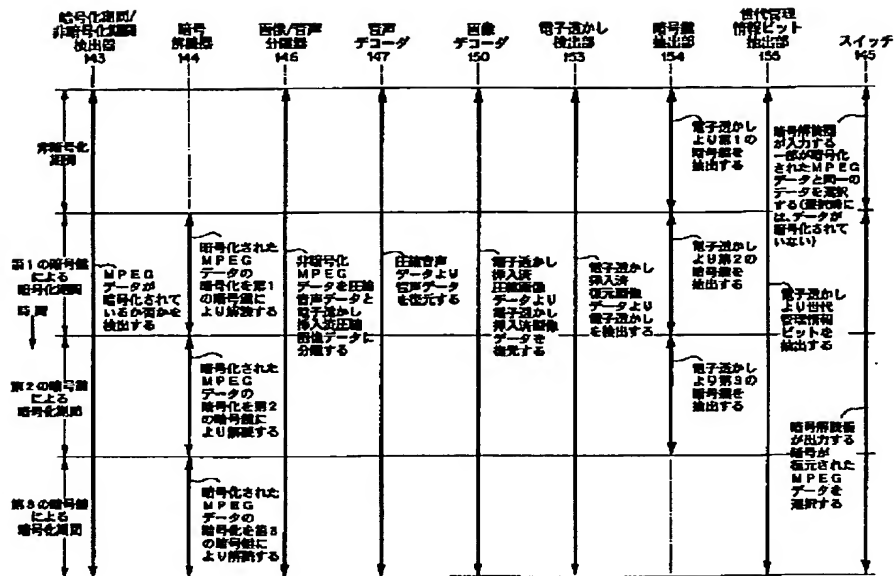
【図9】



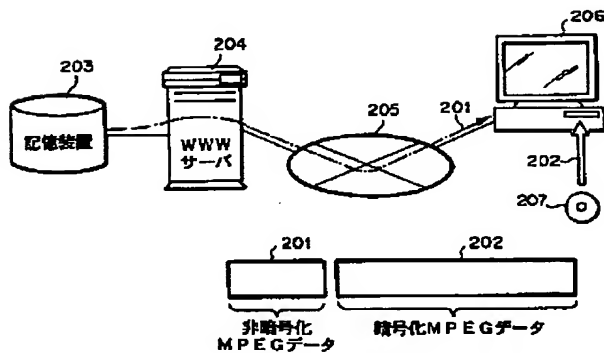
【図7】



【図10】



【図11】



フロントページの続き

(51)Int.Cl.⁷

G 1 1 B 20/10
H 0 4 N 1/387
7/08
7/081
7/167

識別記号

F I

G 1 0 L 9/00
9/18
H 0 4 N 7/08
7/167

テ-マ-ト*(参考)

E 5 D 0 4 5
N 5 J 1 0 4
M
Z
Z

Fターム(参考) 5B057 CA08 CA12 CA16 CB08 CB12
CB16 CC01 CE08
5C063 AB03 AC01 AC05 DA07 DA13
DB09
5C064 CA14 CB01 CC04 CC06
5C076 AA14 BA06
5D044 AB05 AB07 BC03 CC06 DE12
DE50 EF05 FG18 GK08 GK17
GK20 HL11
5D045 DA20
5J104 AA14 NA02